CLAIMS

Sub a1

1. A method of ciphering data transmission in a radio system, comprising:

(602) generating a ciphering key;

(604A) producing a ciphering mask in a ciphering algorithm using the ciphering key as an input parameter;

(606) producing ciphered data by applying the ciphering mask to plain data;

(604B) using a logical channel specific parameter or a transport channel specific parameter as an additional input parameter to the ciphering algorithm.

2. The method as claimed in claim 1, further comprising:

using the direction of transmission as an additional input parameter to the ciphering algorithm.

3. The method as claimed in claim 1, wherein the logical channel specific parameter is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

4. The method as claimed in claim 1, wherein the transport channel specific parameter is a Dedicated Channel Identifier.

5. The method as claimed in claim 1, further comprising:

using a radio frame specific parameter as an additional input parameter to the ciphering algorithm.

6. The method as claimed in claim 5, wherein the radio frame specific parameter is a User Equipment Frame Number.

7. The method as claimed in claim 1, wherein the plain data includes Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and for each logical channel an individual ciphering mask is produced.

8. The method as claimed in claim 7, wherein a Radio Link Control Layer Protocol Data Unit of at least one logical channel is already ciphered, and the step of producing ciphered data is not repeated for said already ciphered Radio Link Control Layer Protocol Data Unit.

9. The method as claimed in claim 1, wherein the plain data includes one Radio Link Control Layer Protocol Data Unit from one logical channel, and for said logical channel an individual ciphering mask is produced.

10. The method as claimed in claim 1, wherein the plain data includes at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask is used in producing the ciphered data.

11. The method as claimed in claim 1, wherein the plain data includes one Transport Block Set including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

12. The method as claimed in claim 1, wherein the plain data includes one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and for each Transport Block Set one ciphering mask is used in producing the ciphered data.

13. The method as claimed in claim 1, wherein the ciphering is performed in the Medium Access Control Layer of a protocol stack.

14. The method as claimed in claim 1, wherein a new ciphering mask is produced for each radio frame of the physical layer of the protocol stack.

15. The method as claimed in claim 1, wherein a new ciphering mask is produced for each interleaving period of the physical layer of the protocol stack.

16. A user equipment (UE), comprising:

generating means (408) for generating a ciphering key (410);

a ciphering algorithm (400) connected with the generating means (408) for producing a ciphering mask (412A, 412B, 412C) using the ciphering key (410) as an input parameter;

ciphering means (416A, 416B, 416C) connected with the ciphering algorithm (400) for producing ciphered data (418A, 418B, 418C) by applying the ciphering mask (412A, 412B, 412C) to plain data (414A, 414B, 414C);

the ciphering algorithm (400) uses a logical channel specific parameter (402A) or a transport channel specific parameter (402B) as an additional input parameter.

17. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) uses the direction of transmission as an additional input parameter.

18. The user equipment as claimed in claim 16, wherein the logical channel specific parameter (402A) is one of the following: a Radio Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

19. The user equipment as claimed in claim 16, wherein the transport channel specific parameter (402B) is a Dedicated Channel Identifier.

20. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) uses a radio frame specific parameter (404) as an additional input parameter.

21. The user equipment as claimed in claim 20, wherein the radio frame specific parameter (404) is a User Equipment Frame Number.

22. The user equipment as claimed in claim 16, wherein the ciphering means (416A, 416B, 416C) accept plain data (414A, 414B, 414C) including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm (400) produces for each logical channel an individual ciphering mask (412A, 412B, 412C), and the ciphering means (416A, 416B, 416C) use for each logical channel the ciphering mask (412A, 412B, 412C) of said channel.

23. The user equipment as claimed in claim 22, wherein a Radio Link Control Layer Protocol Data Unit (414C) of at least one logical channel is already ciphered, and the ciphering means (416C) do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit (414C).

24. The user equipment as claimed in claim 16, wherein the ciphering means (416A) accept plain data (414A) including a Radio Link Control Layer Protocol Data Unit from one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (416A) use for said logical channel the ciphering mask (412A) of said channel.

25. The user equipment as claimed in claim 16, wherein the ciphering means (426) accept plain data including at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (426) use for each Radio Link Control Layer Protocol Data Unit different part of the ciphering mask (412A).

26. The user equipment as claimed in claim 16, wherein the ciphering means (434) accept plain data including one Transport Block Set

including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

27. The user equipment as claimed in claim 16, wherein the ciphering means (434) accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

28. The user equipment as claimed in claim 16, wherein the generating means (408), the ciphering algorithm (400), and the ciphering means (416A, 416B, 416C) reside in the Medium Access Control Layer of a protocol stack.

29. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each radio frame of the physical layer of the protocol stack.

30. The user equipment as claimed in claim 16, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each interleaving period of the physical layer of the protocol stack.

31. A radio network subsystem (RNS), comprising:

generating means (408) for generating a ciphering key (410);

a ciphering algorithm (400) connected with the generating means (408) for producing a ciphering mask (412A, 412B, 412C) using the ciphering key (410) as an input parameter;

ciphering means (416A, 416B, 416C) connected with the ciphering algorithm (400) for producing ciphered data (418A, 418B, 418C) by applying the ciphering mask (412A, 412B, 412C) to plain data (414A, 414B, 414C);

the ciphering algorithm (400) uses a logical channel specific parameter (402A) or a transport channel specific parameter (402B) as an additional input parameter.

32. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) uses the direction of transmission as an additional input parameter.

33. The radio network subsystem as claimed in claim 31, wherein the logical channel specific parameter (402A) is one of the following: a Radio

Access Bearer Identifier, a Logical Channel Identifier, a Signaling Link Identifier.

34. The radio network subsystem as claimed in claim 31, wherein the transport channel specific parameter (402B) is a Dedicated Channel Identifier.

35. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) uses a radio frame specific parameter (404) as an additional input parameter.

36. The radio network subsystem as claimed in claim 35, wherein the radio frame specific parameter (404) is a User Equipment Frame Number.

37. The radio network subsystem as claimed in claim 31, wherein the ciphering means (416A, 416B, 416C) accept plain data (414A, 414B, 414C) including Radio Link Control Layer Protocol Data Units from at least two parallel logical channels, and the ciphering algorithm (400) produces for each logical channel an individual ciphering mask (412A, 412B, 412C), and the ciphering means (416A, 416B, 416C) use for each logical channel the ciphering mask (412A, 412B, 412C) of said channel.

38. The radio network subsystem as claimed in claim 37, wherein a Radio Link Control Layer Protocol Data Unit (414C) of at least one logical channel is already ciphered, and the ciphering means (416C) do not cipher said already ciphered Radio Link Control Layer Protocol Data Unit (414C).

39. The radio network subsystem as claimed in claim 31, wherein the ciphering means (416A) accept plain data (414A) including a Radio Link Control Layer Protocol Data Unit from one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (416A) use for said logical channel theciphering mask (412A) of said channel.

40. The radio network subsystem as claimed in claim 31, wherein the ciphering means (426) accept plain data including at least two successive Radio Link Control Layer Protocol Data Units of one logical channel, and the ciphering algorithm (400) produces for said logical channel an individual ciphering mask (412A), and the ciphering means (426) use for each Radio Link Control Layer Protocol Data Unit a different part of the ciphering mask (412A).

41. The radio network subsystem as claimed in claim 31, wherein the ciphering means (434) accept plain data including one Transport Block Set

including Medium Access Control Layer Protocol Data Units of at least two different logical channels, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

42. The radio network subsystem as claimed in claim 31, wherein the ciphering means (434) accept plain data including one Transport Block Set including a Medium Access Control Layer Protocol Data Unit of one logical channel, and the ciphering algorithm (400) produces for each Transport Block Set an individual ciphering mask (412), and the ciphering means (434) use for each Transport Block Set one ciphering mask (412).

43. The radio network subsystem as claimed in claim 31, wherein the generating means (408), the ciphering algorithm (400), and the ciphering means (416A, 416B, 416C) reside in the Medium Access Control Layer of a protocol stack.

44. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each radio frame of the physical layer of the protocol stack.

45. The radio network subsystem as claimed in claim 31, wherein the ciphering algorithm (400) produces a new ciphering mask (412A, 412B, 412C) for each interleaving period of the physical layer of the protocol stack.